National Institute of Standards and Technology

Briefing for the PITAC

Kevin Mills

January 14, 2000

Presentation Purpose

- At the October 6th interim briefing, we presented a general overview of the NIST NGI program
- Today’s report summarizes our program’s goals, milestones, accomplishments and measured impact.

Presentation Overview

- NIST Role in NGI
- NIST NGI Goals
  - NGI Technologies
  - NGI Security
  - NGI Applications
- NIST NGI Accomplishments
- NIST NGI Plans
- Summary of NGI Requirements for Manufacturing Applications (action item from Oct. 6 PITAC review)
- Summary and Examples of Industry Impact of NIST NGI Program

NIST

NIST Role in the NGI

NIST transfers technology from government-funded research to public standards, industry products and commercial services for the NGI:

- By developing and distributing advanced test and measurement technology and early research prototypes of emerging NGI technology;
- By collaborating with industry to establish standards for the NGI; and,
- By applying emerging NGI technology to assist the U.S. manufacturing sector.

NIST

NGI Technologies Goals

Next-Generation Internet Technologies (Under NGI Goal 1)	
Media Convergence	Develop test and measurement systems to help industry evaluate standards and products aimed at integrating voice, video, and data on the NGI.
Infrastructure Security	Develop standards, reference implementations, and test systems to help industry increase the security of the NGI infrastructure.
Collaborative Systems	Research and develop new test technology for the next generation of multi-party and collaborative NGI applications.
Scalable Systems	Develop reference implementations and test technology to help industry build an NGI infrastructure that will scale to 2^{128} nodes with varying network technologies and with mobile users.

NIST

NGI Security Goals

Security Technologies for the NGI (Under NGI Goal 1)	
Cryptographic Technology and Applications	Work with industry to develop a next-generation advanced encryption standard and to establish technical standards for security services APIs.
Public Key Management	Work with industry to establish effective technical standards for managing public keys.
Security Criteria and Testing	Work with industry to develop a credible and cost-effective system for specifying security criteria and for testing products for compliance.

NIST

NGI Application Goals

Manufacturing Applications (Under NGI Goal 3)	
Requirements Identification and Analysis	Identify NIST manufacturing applications that require advanced networking technologies and services.
Baseline Application Demonstrations	Demonstrate and evaluation manufacturing applications using existing networking technology.
Advanced Application Demonstrations	Demonstrate and evaluate manufacturing applications in increments, as new NGI capabilities are created.

NIST NGI Technologies Accomplishments

Next-Generation Internet Technologies (Under NGI Goal 1) **Media Convergence (1 of 3)**	
Internet Quality of Service	FY98Q1 – Release of **ISPI** – IntServ, RSVP, RTP experimentation and testing tool FY98Q2 – Initial release of **NISTNet**– network emulation, QoS sensitivity analysis tool FY99Q2 – Release of **DIPPER** – system for distributed testing of QoS routing and signaling protocols. FY99Q2 – Initial release of **NIST Switch** – research platform for MPLS / QoS routing.

NGI Technologies Accomplishments

Next-Generation Internet Technologies (Under NGI Goal 1)

Media Convergence (2 of 3)

High Speed Backbone Networks – including: **Asynchronous Transfer Mode (ATM)** **and** **Wave-Division Multiplexing (WDM)**	Developed the **NIST ATM network simulator** to evaluate proposed traffic management schemes and PNNI routing techniques. FY99Q4 – Released **MERLin** –WDM design and hybrid analytical/simulation modeling environment. Published results on the performance comparison of various traffic management schemes proposed to the industry’s ATM Forum.. Published reports on performance comparison of various PNNI routing schemes proposed to the ATM Forum.

NGI Technologies Accomplishments

<table>
<tr><th colspan="2">Next-Generation Internet Technologies (Under NGI Goal 1)
Media Convergence (3 of 3)</th></tr>
<tr><td><b>Hybrid Fiber-Coax Access to the Home</b></td><td>Enhanced the <b>NIST ATM network simulator</b> to include HFC network protocols, IEEE802.14 & SCTE.
Published results on contention resolution algorithms, bandwidth allocation, and priority schemes, on end-to-end performance issues for TCP/IP, ATM traffic control.
Published reports on performance comparison of IEEE 802.14 and SCTE MAC protocols, and on support of IP QoS on HFC.
Authored conformance requirements (Annex B) of the IEEE 802.14 standard.</td></tr>
</table>

NGI Technologies Accomplishments

Next-Generation Internet Technologies (Under NGI Goal 1) Infrastructure Security	
IPsec	FY98Q1 – Initial release of **Cerberus** – IPsec reference implementation FY98Q2 – **IPsec-WIT** announced – WWW based, on-line interoperability tester for IETF IPSec protocols. FY99Q2 – Initial release of **Cerberus/PlutoPlus** – integrated IPSec + IKE reference implementation. FY99Q3 – **IPSec-WIT** upgraded – with key management testing.

NGI Technologies Accomplishments

<table>
<tr><th colspan="2">Next-Generation Internet Technologies (Under NGI Goal 1)
Collaborative Systems and Scalable Systems</th></tr>
<tr><td><b>Distributed Multi-Party Test Technology</b></td><td>FY98Q3 – Initial release of <b>AGNI</b> – applied to test MASH and CVW, two next-generation Internet-based, multi-party, multimedia collaborative systems
FY99Q3 – Second release of <b>AGNI</b> – as a general middleware toolkit for reconfigurable distributed systems</td></tr>
<tr><td><b>IP version 6</b></td><td>FY98 – Release of LibpcapV6, protocol testing tools for IPv6.</td></tr>
</table>

NIST

NGI Security Accomplishments

Security Technologies for the NGI (Under NGI Goal 1) Cryptographic Technology and Applications	
Advanced Encryption Standard (AES)	FY97 drafted evaluation and submission criteria FY97 called for candidate algorithms FY98 candidate algorithm submissions FY99 selected final candidates (5)
Cryptographic Module Validation	FY98 ANSI CMV standards initiated FY98 Five-year review cycle of FIPS 140-1 FY98 RFC Federal Register Notice issued in Oct., FY99 comments received Jan.1999

NGI Security Accomplishments

Security Technologies for the NGI (Under NGI Goal 1) **Public Key Management**	

Public Key Infrastructure (PKI)	FY97 completed Minimum Interoperability Specification for PKI Components (MISPC)
	FY98 developed MISPC Reference Implementation;
	FY98 developed MISPC with confidentiality support;
	FY98 developed security requirements for CAs
	FY99 released MISPC Reference Implementation;
	FY99 developed MISPC Confidentiality Extensions;
	FY99 conducted interoperability demonstration

NGI Security Accomplishments

Security Technologies for the NGI (Under NGI Goal 1) Security Criteria and Testing	
National Information Assurance Partnership (NIAP)	FY97 completed draft specification of Common Criteria for security evaluation and testing FY99 signed an international mutual recognition arrangement regarding the Common Criteria FY99 Common Criteria becomes international standard (ISO/IEC 15408) FY99 Testing Laboratory Accreditation Begins

NGI Application Accomplishments

Manufacturing Applications (Under NGI Goal 3)	
Manufacturing Collaboratories	FY99 Manufacturing collaboratory for robotic arc welding became operational. FY99 Established partnerships with Borg-Warner Automotive and University of Michigan for deployment of collaboratory in support of new clutch product being designed with BWA groups in U.S. and Germany
Manufacturing Virtual Interfaces	FY99 Demonstrated remote-controlled monitoring of hexapod machine tool FY00 (November) Demonstrated multi-user, multi-media virtual environment for monitoring and control of welding robot

NIST

NGI Technologies Plans

Next-Generation Internet Technologies (Under NGI Goal 1) **Media Convergence and Infrastructure Security**	
Internet Quality of Service	FY00-FY01 – Evaluation of MPLS-enabled routing and signaling mechanisms to support QoS and virtual network infrastructures
Wave-Division Multiplexing	FY00-01 – Evaluation of wave length assignment and routing algorithms and proposals for mapping IP to wavelengths
IP and DNS Security	FY00-01 – Design and testing of integrated security management systems IPSec+IKE+PKIX, policy management, security systems simulations, AES support, and DNS Sec test tools

NGI Technologies Plans

Next-Generation Internet Technologies (Under NGI Goal 1) **Scalable Systems**	
Agile Networking Infrastructures	FY00-01 – Research and development of resource control techniques for active networks technologies FY00-01 – Research and development of networking technologies for pervasive / home computing environments.
Wireless Communications	FY00 – Release software test workbench for IMT-2000 evaluations FY00 – Develop formal model of Bluetooth link layer and evaluate the specification FY00 – Develop and validate channel models for LMDS FY00 – Evaluate the ability of IMT-2000 technology to carry video traffic

NGI Security Plans

Security Technologies for the NGI (Under NGI Goal 1) Cryptographic Technology and Applications	
Advanced Encryption Standard (AES)	FY00 select final algorithms FY01 publish AES standard FY01 publish Modes of Operation standard FY01 validation tests available in labs
Cryptographic Module Validation	FY00 Completion of FIPS 140-2 update FY00 Testing by labs for FIPS 140-2 FY02 ANSI CMV standard

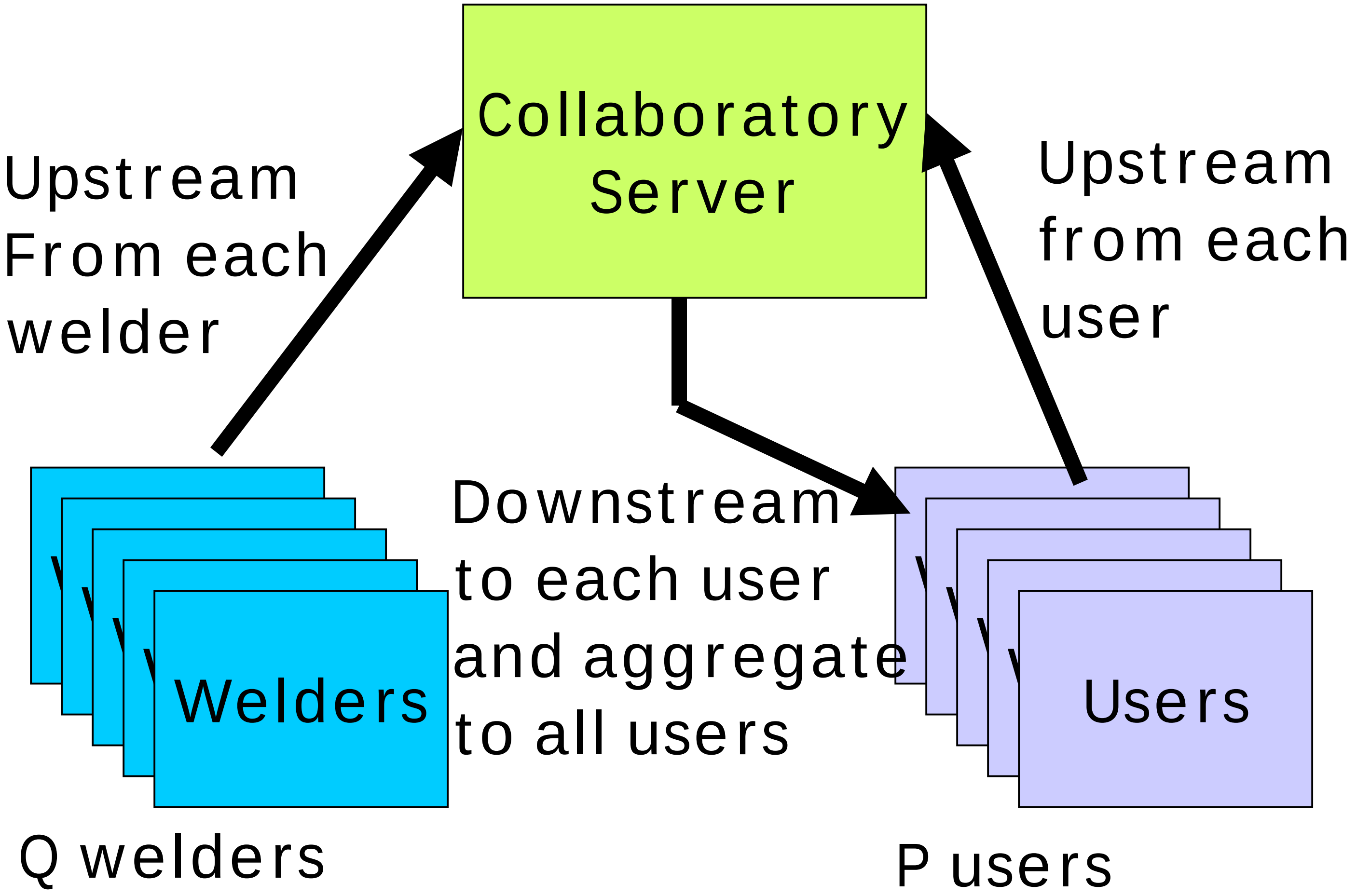
NGI Security Plans

Security Technologies for the NGI (Under NGI Goal 1) Public Key Management and Security Criteria and Testing	
Public Key Infrastructure (PKI)	FY00 Complete MISPC V2 FY00 develop Protection Profile (PP) for Certificate Issuing and Management Components (CIMCs), FY00 develop Federal certificate profile FY01 Develop MISPC V2 Reference Implementation FY01 develop design test requirements for CIMC PP
National Information Assurance Partnership (NIAP)	FY00 Common Criteria Evaluation and Validation Program Operational

NGI Application Plans

Manufacturing Applications (Under NGI Goal 3)	
NGI Manufacturing Applications Work Ceases After FY00	NIST effort supporting NGI Applications Thrust for FY01 and beyond is being reprogrammed toward Software Design and Productivity. Without the availability of the NGI infrastructure to commercial manufacturers the NGI Applications Thrust is not considered critical to the NIST mission with respect to the American manufacturing industry.

Architecture for Welding Collaboratory Application



Collaboratory Server

Upstream From each welder

Upstream from each user

Downstream to each user and aggregate to all users

Welders

Users

Q welders

P users

Ideal Networking Requirements for Welding Collaboratory Application

Upstream Requirements from User Client to Server Total is 3.1 Gbps per user	
User State	**50 kbps (50 frames/s X 1 kbp/frame user state data)**
User Audio	**80 kbps (user audio upstream)**
Four live video feeds from the welding laboratory	**3 Gbps (4 video feeds from the welding lab, assuming 2:1 compression of 60 Hz 1kX1k images, because pipeline latencies and image mapping in virtual world rule out streaming)**

Idea Networking Requirements for Welding Collaboratory Application

Upstream Requirements from Welder Client to Server Total is 1.33 Mbps per Welder	
Robot Control and Feedback Signals	**50 kbps**
Measured Weld Quality	**1.2 Mbps**

Idea Networking Requirements for Welding Collaboratory Application

Downstream Requirements from Server to Each User 3 + [0.13*(P-1) + 1.3*Q]*10**(-3) Gbps per user with P users and Q welders	
Video	3 Gbps
State and Audio of P-1 other users	(P-1)*130 kbps
Welder and Robot Data from Q welders	Q*1.3 Mbps

Total downstream from server:

P * { 3 + [0.13*(P-1) + 1.3*Q]*10(-3) } Gbps**

for P users and Q welders

Comments on Latency, Jitter & Synchronization for Welding Application

- **Important issues for audio, button-pushing, and video**
- **Requirements are for low latency, low jitter, and tight synchronization (e.g., a few ms each)**
- **If video is only a confirmation of model’s actions, then greater latency is tolerable**

NIST Industry Impact of NIST QoS Project

- **Delivering Tools & Prototypes**
  - **NIST Net**
  - **ISPI**
  - **DIPPER**
  - **NIST Switch**
- **Wide Industry use for:**
  - **protocol testing (RSVP, VOIP)**
  - **QoS research**
  - **application design**
  - **usability analysis**
  - **pilot deployment testing**

- **Customers:**
  - **100's of organizations acquired our tools, including:**
  - **3Com, Ascend, @Home, AT&T research, Bay Networks, Bell Atlantic, Boeing, BT, Cisco, Compaq, DirectTV, GTE labs, Ericsson radio, Fore, HP, IBM, Intel, LBL, Lucent, Microsoft, Motorola, Nortel, NIMA, Nokia, Radical Entertainment, Sony, US West.**

Industry Impact of NIST IP sec Project

- **Tools, Prototypes and Specs**
  - **Cerberus / PlutoPlus**
  - **IPsec WIT**
  - **IETF specifications**
- **Wide Industry use for:**
  - **protocol testing**
  - **implementation reference**
  - **IPsec research**
  - **pilot deployment testing**

- **Customers:**
  - **100's of organizations acquired our tools, including:**
  - **Microsoft, Lucent, Intel, Cisco, Sun MS, MCI, IBM, MIT, Bay Networks, TIS, SRI Int, BBN, DEC, Secure Computing, NRL, Smart Card Developer Association, Shiva, Epic, Mentat, USAF**

Summary

NIST transfers technology from government-funded research to commercial products and services for the NGI:

- By developing and distributing advanced test and measurement technology and early research prototypes of emerging NGI standards
- By collaborating with industry to establish standards for the NGI
- By applying emerging NGI technology to assist the U.S. manufacturing sector